UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/072,840	02/06/2002	Steven Charles Glassman	9772-0313-999	3725

22879 7590 09/08/2005

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
MIZAN, SHAHIN	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 09/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/072,840	GLASSMAN ET AL.	
	Examiner	Art Unit	
	Shahin Mizan	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 February 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-55* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-55* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 February 2002* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-55 have been examined.

Drawings

2. The drawings are objected to because paragraph [0022] refers to a login token but no reference to a login token is made in Fig. 3A. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

The disclosure is objected to because of the following informalities:

a. Paragraph [0026]/line 2 - "**130**" should be changed to "**132**"

b. Paragraph [0026]/line 3 - "**130**" should be changed to "**132**"

c. Paragraph [0027]/line 7 - "**132**" should be changed to "**130**"

d. Paragraph [0027]/line 8 - "**132**" should be changed to "**130**"

e. Paragraph [0027]/line 10 - "**132**" should be changed to "**130**"

f. Paragraph [0027]/line 12 - "**132**" should be changed to "**130**"

g. Paragraph [0027]/line 14 - "**132**" should be changed to "**130**"

Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-8, 11-13, 15-34, and 42-55 are rejected under 35 U.S.C. 102(b) as being anticipated by Sandhu et al. (US Patent No. 6,883,095).

As per independent claim 1, Sandhu et al. teaches a login method comprising processing a login token, if provided, during a login attempt, wherein the login attempt

is impermissible, and thus unsuccessful, if the login attempt occurs before expiration of a first period of time following an unsuccessful login attempt associated with said login token *(note column 10, line 45 - logged-in ticket is a login token processed by a server when presented at a login session; also note column 6, lines 54 - 66 - first period of time described)*; and

providing an updated login token in response to the login attempt, wherein the updated login token does not permit a subsequent login attempt before expiration of a second period of time if the login attempt is unsuccessful *(note column 60 - second challenge is the updated login token)*.

As per claim 2, which is dependent on claim 1, Sandhu et al. teaches the login method of claim 1, further comprising maintaining a login-attempt success indicator, said login-attempt success indicator indicating whether the login attempt is successful, said login-attempt success indicator being referenced during the subsequent login attempt *(note Fig. 10 - box identified as 1225 performs this function)*.

As per claim 3, which is dependent on claim 2, Sandhu et al. teaches the login method of claim 2, further comprising including in the updated login token an attempt success indicator, said attempt success indicator indicating whether the login attempt is successful, said attempt success indicator being referenced during the subsequent login attempt *(note Fig. 10 - box identified as 1245 performs the function of updated login token)*.

As per claim 4, which is dependent on claim 3, Sandhu et al. teaches the login method of claim 3, wherein the login-attempt success indicator is a login class, wherein the login class is first-class if the login attempt is successful attempt *(note column 11, line 9 - item 1035 is the success indicator)*.

As per claim 5, which is dependent on claim 1, Sandhu et al. teaches the login method of claim 1, further comprising maintaining a time stamp, said time stamp corresponding to the second period of time *(note Fig. 8 - time and date information associated with a particular login attempt is recorded)*.

As per claim 6, which is dependent on claim 1, Sandhu et al. teaches the login method of claim 1, further comprising inserting in the updated login token a time stamp, said time stamp corresponding to the second period of time *(note Fig. 8 - time and date information associated with a particular login attempt is recorded)*.

As per claim 7, which is dependent on claim 1, Sandhu et al. teaches the login method of claim 1, further comprising maintaining an account identifier, said account identifier corresponding to an account that is the subject of the login attempt, wherein the subsequent login attempt is impermissible if an account that is the subject of the subsequent login attempt does not correspond to the account identifier *(note Fig. 10 - the box labeled 1215 implies an account associated with each user)*.

As per claim 8, which is dependent on claim 1, Sandhu et al. teaches the login method of claim 1, further comprising inserting in the updated login token an account identifier, said account identifier corresponding to an account that is the subject of the login attempt, wherein the subsequent login attempt is impermissible if an account that is the subject of the subsequent login attempt does not correspond to the account identifier *(note Fig. 10 - the box labeled 1215 implies an account associated with each user)*.

As per claim 11, which is dependent on claim 1, Sandhu et al. teaches the login method of claim 1, further comprising maintaining a password identifier, said password

identifier corresponding to a password submitted with the login attempt, wherein the subsequent login attempt is impermissible if a password submitted with the subsequent login attempt does not correspond to the password identifier *(note Fig. 8 – user ID and password information associated with a particular login attempt is established in the server; also note Fig. 10 – box labeled 1215 deals with password identifier)*.

As per claim 12, which is dependent on claim 1, Sandhu et al. teaches the login method of claim 1, further comprising inserting in the updated login token a password identifier, said password identifier corresponding to a password submitted with the login attempt, wherein the subsequent login attempt is impermissible if a password submitted with the subsequent login attempt does not correspond to the password identifier *(note Fig. 8 – user ID and password information associated with a particular login attempt is established in the server; also note Fig. 10 – box labeled 1215 deals with password identifier)*.

As per claim 13, which is dependent on claim 1, Sandhu et al. teaches the login method of claim 1, further comprising inserting in the updated login token a validity stamp, said validity stamp designed to prevent the use of an invalid login token, wherein the login attempt is impermissible if the login token does not include a valid validity stamp *(note Fig. 10 – box labeled 1215 provides validity stamp)*.

As per claim 15, which is dependent on claim 1, Sandhu et al. teaches the login method of claim 1, further comprising maintaining a count of unsuccessful login attempts *(note Fig. 9 - box identified as 1220 performs this function; also note Fig. 10 – box identified as 1225)*.

As per claim 16, which is dependent on claim 15, Sandhu et al. teaches the login method of claim 15, further comprising incrementing the count if the login attempt is impermissible *(note Fig. 10 - box identified as 1225 performs this function)*.

As per claim 17, which is dependent on claim 15, Sandhu et al. teaches the login method of claim 15, further comprising incrementing the count if the login attempt is permissible but otherwise unsuccessful *(note Fig. 10 - box identified as 1225 performs this function)*.

As per claim 18, which is dependent on claim 15, Sandhu et al. teaches the login method of claim 15, further comprising selecting the second period of time by reference to the count, wherein the second period of time is longer than it otherwise would be if the count reaches a predefined threshold *(note Fig. 11 - box identified as 1301 performs this function)*.

As per claim 19, which is dependent on claim 15, Sandhu et al. teaches the login method of claim 15, further comprising selecting the second period of time by reference to the count, wherein the second period of time is longer than it otherwise would be if the count reaches a predefined threshold within a third period of time *(note Fig. 11 - box identified as 1301 performs this function)*.

As per claim 20, which is dependent on claim 1, Sandhu et al. teaches the login method of claim 1 *(see above)*, wherein the login attempt is impermissible if the login token is not provided during the login attempt *(note column 11, lines 31 - 37 – logged-in ticket equates to a token containing time stamp and random number R1 information is required otherwise the login attempt is impermissible)*.

As per claim 21, which is dependent on claim 1, Sandhu et al. teaches the login method of claim 1, further comprising maintaining a count of unsuccessful login attempts to login with a password *(note Fig. 10 - box identified as 1225 performs this function)*.

As per claim 22, which is dependent on claim 21, Sandhu et al. teaches the login method of claim 21, further comprising incrementing the count if the login attempt is impermissible and is made with the password *(note Fig. 10 - box identified as 1225 performs this function)*.

As per claim 23, which is dependent on claim 21, Sandhu et al. teaches the login method of claim 21, further comprising incrementing the count if the login attempt is permissible but otherwise unsuccessful and is made with the password *(note Fig. 10 - box identified as 1225 performs this function)*.

As per claim 24, which is dependent on claim 21, Sandhu et al. teaches the login method of claim 21, further comprising selecting the second period of time by reference to the count, wherein the second period of time is longer than it otherwise would be if the count reaches a predefined threshold and the login attempt is made with the password *(note Fig. 11 - box identified as 1301 performs this function)*.

As per claim 25, which is dependent on claim 21, Sandhu et al. teaches the login method of claim 21, further comprising selecting the second period of time by reference to the count, wherein the second period of time is longer than it otherwise would be if the count reaches a predefined threshold within a third period of time and the login attempt is made with the password *(note Fig. 11 - box identified as 1301 performs this function)*.

As per claim 26, which is dependent on claim 21, Sandhu et al. teaches the login method of claim 21, wherein the second period of time is not increased as the count increases unless each of the defined number of unsuccessful login attempts to login with the password occur within a third period of time *(note column 15, lines 6 - 8 – the time is variable meaning keeping it the same or increased or decreased)*.

As per claim 27, which is dependent on claim 21, Sandhu et al. teaches the login method of claim 21, further comprising invalidating the subsequent login attempt if the count equals a predefined threshold and the password is submitted with the subsequent login attempt *(note Fig. 10 - box identified as 1235 performs this function)*.

As per claim 28, which is dependent on claim 1, Sandhu et al. teaches the login method of claim 1, further comprising maintaining a count of unsuccessful login attempts to login with a user name *(note Fig. 9 - box identified as 1120 performs this function)*.

As per claim 29, which is dependent on claim 28, Sandhu et al. teaches the login method of claim 28, further comprising incrementing the count if the login attempt is impermissible *(note Fig. 10 - box identified as 1225 performs this function)*.

As per claim 30, which is dependent on claim 28, Sandhu et al. teaches the login method of claim 28, further comprising incrementing the count if the login attempt is permissible but otherwise unsuccessful *(note Fig. 10 - box identified as 1225 performs this function)*.

As per claim 31, which is dependent on claim 28, Sandhu et al. teaches the login method of claim 28, further comprising selecting the second period of time by reference to the count, wherein the second period of time is longer than it otherwise would be if

the count reaches a predefined threshold and the login attempt is made with the user name *(note Fig. 11 - box identified as 1301 performs this function)*.

As per claim 32, which is dependent on claim 28, Sandhu et al. teaches the login method of claim 28, further comprising selecting the second period of time by reference to the count, wherein the second period of time is longer than it otherwise would be if the count reaches a predefined threshold within a third period of time and the login attempt is made with the user name *(note column 15, lines 6 - 8 – the time is variable)*.

As per claim 33, which is dependent on claim 28, Sandhu et al. teaches the login method of claim 28, wherein the second period of time is not increased as the count increases unless each of the defined number of unsuccessful login attempts to login with the user name occur within a third period of time *(note column 15, lines 6 - 8 – the time is variable)*.

As per claim 34, which is dependent on claim 28, Sandhu et al. teaches the login method of claim 28, further comprising invalidating the subsequent login attempt if the count equals a predefined threshold and the user name is submitted with the subsequent login attempt *(note column 15, line 15 – pre established threshold limit described)*.

As per claim 42, which is dependent on claim 1, Sandhu et al. teaches the login method of claim 1, wherein the second period of time is a first length if the login attempt is one in a series of unsuccessful login attempts associated with the login token, which follow a successful attempt associated with the login token, if the series of unsuccessful login attempts does not include more than a predefined number unsuccessful login attempts *(note Fig. 10 - box identified as 1230 and 1235 performs this function)*;

the second period of time is a second length if the login attempt is one in a series of unsuccessful login attempts associated with the login token, which follow a successful attempt associated with the login token, if the series of unsuccessful login attempts includes the predefined number unsuccessful login attempts *(note Fig. 10 - box identified as 1230 and 1235 performs this function)*;

the second period of time is a third length if the login attempt does not follow a successful attempt associated with the login token, said third length exceeding the first length *(note Fig. 10 - box identified as 1230 and 1235 performs this function)*; and

the second period of time is a fourth length if the login token is not provided during the login attempt, said fourth length exceeding the first length *(note Fig. 10 - box identified as 1230 and 1235 performs this function)*.

As per claim 43, which is dependent on claim 1, Sandhu et al. teaches the login method of claim 1, further comprising processing a second login token, if provided, during a second login attempt, wherein the login cookie provided in response to the second login attempt does not permit a subsequent login attempt at least until the second period of time has expired twice since the login attempt name *(note column 15, lines 6 - 8)*.

As per independent claim 44, Sandhu et al. teaches a login method comprising processing a login attempt to determine whether the login attempt is successful, said login attempt being successful if permissible and submitted with a valid user name and password combination *(note column 10, line 17 and lines 47 - 50)*;

providing a first-class login token if the login attempt is successful, said first-class login token permitting a predefined number of unsuccessful login attempts without imposing more than a first time delay between each of said unsuccessful login attempts *(note column 6, lines 2 - 3 - first challenge equates to first class login; also note column 13, line 54 - indication field can include data that may allow the user with subsequent login attempt without immediately going to the second challenge)*;

providing a second-class login token if the login attempt is unsuccessful and a login token submitted with the login request is second-class, wherein a subsequent login attempt made with said second-class login token is not permissible if submitted prior to expiration of a second time delay, said second time delay exceeding said first time delay *(note column 6, line 10 - second challenge equates to second class login; also note Fig. 8 and 11)*;

providing the second-class login token if the login attempt is unsuccessful and is the last of a series of unsuccessful login attempts associated with a first-class login token, said series including more than the predefined number of unsuccessful login delay *(note column 6, line 10 - second challenge equates to second class login; also note Fig. 8 and 11; also note column 13, line 54 - indication field can include data that may allow the user with subsequent login attempt for certain threshold count before going to the second challenge)*; and

providing the second-class login token if a login token is not submitted with the login attempt, said login attempt not being permissible *(note column 10, lines 47 - 50 – the function performed in the absence of logged-in ticket is described)*.

As per claim 45, which is dependent on claim 44, Sandhu et al. teaches the login method of claim 44, wherein the login attempt is not permissible if a login token

submitted with said login attempt is invalid *(note column 11, line 57 - login with invalid logged-in ticket is not allowed)*.

As per claim 46, which is dependent on claim 44, Sandhu et al. teaches the login method of claim 44, wherein the login attempt is not permissible if said login attempt is made prior to expiration of a time delay associated with a login token submitted with said login attempt *(note column 14, lines 9 - 14 - login attempt prior to the expiration of the delay is not permissible)*.

As per independent claim 47, Sandhu et al. teaches a computer program product for use in conjunction with a computer system, the computer program product comprising a computer readable storage medium and a computer program mechanism embedded therein, the computer program mechanism comprising:

instructions for processing a login attempt to determine whether the login attempt is successful, said login attempt being successful if permissible and submitted with a valid user name and password combination *(note column 8, lines 31 - 41; also note column 9, lines 2 - 3; also note Fig. 4,5,6, and 7)*;

instructions for providing a first-class login token if the login attempt is successful, said first-class login token permitting a predefined number of unsuccessful login attempts without imposing more than a first time delay between each of said unsuccessful login attempts combination *(note column 8, lines 31 - 41; also note column 9, lines 2 - 3; also note Fig. 4,5,6, and 7)*;

instructions for providing a second-class login token if the login attempt is unsuccessful and a login token submitted with the login request is second-class,

wherein a subsequent login attempt made with said second-class login token is not permissible if submitted prior to expiration of a second time delay, said second time delay exceeding said first time combination *(note column 8, lines 31 - 41; also note column 9, lines 2 - 3; also note Fig. 4,5,6, and 7)*;

instructions for providing the second-class login token if the login attempt is unsuccessful and is the last of a series of unsuccessful login attempts associated with a first-class login token, said series including more than the predefined number of unsuccessful login attempts combination *(note column 8, lines 31 - 41; also note column 9, lines 2 - 3; also note Fig. 4,5,6, and 7)*; and

instructions for providing the second-class login token if a login token is not submitted with the login attempt, said login attempt not being permissible combination *(note column 8, lines 31 - 41; also note column 9, lines 2 - 3; also note Fig. 4,5,6, and 7)*.

As per independent claim 48, Sandhu et al. teaches a computer program product for use in conjunction with a computer system, the computer program product comprising a computer readable storage medium and a computer program mechanism embedded therein, the computer program mechanism comprising:

instructions for processing a login token, if provided, during an attempt to login, wherein the login attempt is impermissible if the login attempt occurs before expiration of a first period of time following an unsuccessful login attempt associated with said login token *(note Fig. 1,4,5,6, and 7; also note column 9, lines 4 - 6 - software necessary for the invention is described; also note Fig. 2A - box 415 and step 510 perform this function)*; and

instructions for providing an updated login token in response to the login attempt, wherein the updated login token does not permit a subsequent login attempt before expiration a second period of time if the login attempt is impermissible token *(note Fig. 1,4,5,6, and 7; also note column 9, lines 4 - 6 - software necessary for the invention is described; also note Fig. 2A - box 415, 420, 425, 430, and 435 perform this function)*.

As per independent claim 49, Sandhu et al. teaches a computer system for processing login requests, comprising:

a first-class login server and a second-class login server, said first-class login server and said second-class login server each including a storage unit and a processor, said storage unit configured to store login information, said processor configured to process login requests with reference to said login information *(note Fig. 6 and 7 – server performing these functions is shown; also note Fig. 4 and 5 - second class login server function can be done here; also note column 9, line 20 - additional server that can perform any one of the server classes function is allowable)*;

the first-class login server and the second-class login server each configured to process a login attempt to determine whether the login attempt is successful, said login attempt being successful if permissible and submitted with a valid user name and password combination *(note Fig. 6 and 7 – server performing these functions is shown; also note Fig. 4 and 5 - second class login server function can be done here; also note column 9, line 20 - additional server that can perform any one of the server classes function is allowable)*;

the first-class login server configured to process login attempts made with a first-class login token and the second-class login server configured to process login attempts made with a second-class login token *(note Fig. 6 and 7 – server performing these*

functions is shown; also note Fig. 4 and 5 - second class login server function can be done here; also note column 9, line 20 - additional server that can perform any one of the server classes function is allowable);

the first-class login server and the second-class login server each further configured to provide a first-class login token if the login attempt is successful, said first-class login token permitting a predefined number of unsuccessful login attempts without imposing more than a first time delay between each of said unsuccessful login attempts *(note Fig. 6 and 7 – server performing these functions is shown; also note Fig. 4 and 5 - second class login server function can be done here; also note column 9, line 20 - additional server that can perform any one of the server classes function is allowable)*;

the second-class login server further configured to provide a second-class login token if the login attempt is unsuccessful, wherein a subsequent login attempt made with said second-class login token is impermissible if submitted prior to expiration of a second time delay, said second time delay exceeding said first time delay *(note Fig. 6 and 7 – server performing these function is shown; also note Fig. 4 and 5 - second class login server function can be done here; also note column 9, line 20 - additional server that can perform any one of the server classes function is allowable)*; and

the first-class login server further configured to provide a second-class login token if the login attempt is unsuccessful and the login attempt is the last of a series of unsuccessful login attempts associated with a specific first-class login token, said series including more than the predefined number of unsuccessful login attempts *(note Fig. 6 and 7 – server performing these functions is shown; also note Fig. 4 and 5 - second class login*

server function can be done here; also note column 9, line 20 - additional server that can perform any one of the server classes function is allowable).

As per claim 50, which is dependent on claim 49, Sandhu et al. teaches the computer system of claim 49, wherein the second-class login server is further configured to serially process login attempts *(note Fig. 2A, 2B, 2C, 3A, and 3 - serial login process described; also note Summary Disclosure of the Invention).*

As per claim 51, which is dependent on claim 50, Sandhu et al. teaches the computer system of claim 50, wherein the second-class server is further configured to process login attempts at a defined rate *(note Fig. 8 – shows the defined rate).*

As per claim 52, which is dependent on claim 51, Sandhu et al. teaches the computer system of claim 51, wherein the second-class server is further configured to decrease the defined rate in response to an occurrence of a set of unsuccessful login attempts *(note Fig. 11 – shows the decreased defined rate).*

As per claim 53, which is dependent on claim 51, Sandhu et al. teaches the computer system of claim 51, wherein the second-class server is further configured to decrease the defined rate if a defined number of unsuccessful login attempts occur during a defined period of time *(note column 6, lines 18 - 20 - the invention allows for modification of pre-set maximum to include higher delay rate of processing prior to the attainment of the threshold; also note Fig. 9).*

As per claim 54, which is dependent on claim 53, Sandhu et al. teaches the computer system of claim 53, wherein the second-class server is further configured to increase the defined rate if the defined number of unsuccessful login attempts do not occur during the defined period of time *(note column 6, lines 18 - 20 - the invention allows for*

modification of pre-set maximum to include higher delay rate of processing prior to the attainment of the threshold; also note Fig. 9).

As per claim 55, which is dependent on claim 49, Sandhu et al. teaches the computer system of claim 49, wherein the first-class login server is the default login server such that all login attempts are initially processed by said first-class login server, which is configured to redirect login attempts made with a second-class login token to the second-class login server *(note Fig. 6 – the default server is the first class login server as shown; also note column 10, lines 51 - 58 - default server can use other computer to perform the second login attempt).*

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 9, 10, 14, and 35-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sandhu et al. as applied to claim 1 above, and further in view of Bachman et al. (US Patent No. 5,907,621).

Sandhu et al. differs from the claimed invention in that he teaches a login method comprising processing and updating a login token but fails to specify the limitations below. Bachman et al., however, does teach these limitations in a method similar to that of Sandhu et al.

As per claim 9, which is dependent on claim 1, Bachman et al. teaches the login method of claim 1, further comprising maintaining a network address identifier, said network address identifier corresponding to a network address from which the login attempt originates, wherein the subsequent login attempt is impermissible if a network address from which the subsequent login attempt originates does not correspond to the network address identifier *(note column 3, line 48 - IP address is part of the session table)*.

As per claim 10, which is dependent on claim 1, Bachman et al. teaches the login method of claim 1, further comprising inserting in the updated login token a network address identifier, said network address identifier corresponding to a network address from which the login attempt originates, wherein the subsequent login attempt is impermissible if a network address from which the subsequent login attempt originates does not correspond to the network address identifier *(note column 3, line 48 - IP address is part of the session table)*.

As per claim 14, which is dependent on claim 1, Bachman et al. teaches the login method of claim 1, further comprising inserting in the updated login token a nonce, said nonce designed to prevent the reuse of an otherwise valid login token, wherein the login attempt is impermissible if the login token does include a nonce used in a prior login attempt *(note column 3, lines 34 - 40 – random session token is equivalent to nonce; also note column 5, line 32)*.

As per claim 35, which is dependent on claim 1, Bachman et al. teaches the login method of claim 1, further comprising maintaining a count of unsuccessful login

attempts to login from a network address *(note column 3, line 48 - IP address is part of the session table; also note column 4, lines 43 - 49).*

As per claim 36, which is dependent on claim 35, Bachman et al. teaches the login method of claim 35, further comprising incrementing the count if the login attempt is impermissible and made from the network address *(note column 3, line 48 - IP address is part of the session table; also note column 4, lines 43 - 49).*

As per claim 37, which is dependent on claim 35, Bachman et al. teaches the login method of claim 35, further comprising incrementing the count if the login attempt is permissible but otherwise unsuccessful and made from the network address *(note column 3, line 48 - IP address is part of the session table; also note column 4, lines 43 - 49).*

As per claim 38, which is dependent on claim 35, Bachman et al. teaches the login method of claim 35, further comprising selecting the second period of time by reference to the count, wherein the second period of time is longer than it otherwise would be if the count reaches a predefined threshold and the login attempt is made from the network address *(note column 3, line 48 - IP address is part of the session table; also note column 4, lines 43 - 49).*

As per claim 39, which is dependent on claim 35, Bachman et al. teaches the login method of claim 35, further comprising selecting the second period of time by reference to the count, wherein the second period of time is longer than it otherwise would be if the count reaches a predefined threshold within a third period of time and the login attempt is made from the network address *(note column 3, line 48 - IP address is part of the session table; also note column 4, lines 43 - 49).*

As per claim 40, which is dependent on claim 35, Bachman et al. teaches the login method of claim 35, wherein the second period of time is not increased as the count increases unless each of the defined number of unsuccessful login attempts to login from the network address occur within a third period of time *(note column 3, line 48 - IP address is part of the session table; also note column 4, lines 43 - 49)*.

As per claim 41, which is dependent on claim 35, Bachman et al. teaches the login method of claim 35, further comprising invalidating the subsequent login attempt if the count equals a predefined threshold and the subsequent login attempt is made from the network address *(note column 3, line 48 - IP address is part of the session table; also note column 4, lines 43 - 49)*.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Sandhu et al.'s method such that the limitations taught by Bachman et al. are included, since Bachman et al. teaches these limitations within the same field of endeavor (*preventing dictionary/replay attack*) and with the same problem sought to be solved *(promoting secure, authorized access attempts and inhibiting illegal access/attempts, note column 1, lines 13-21 and column 2, lines 10-20)*.

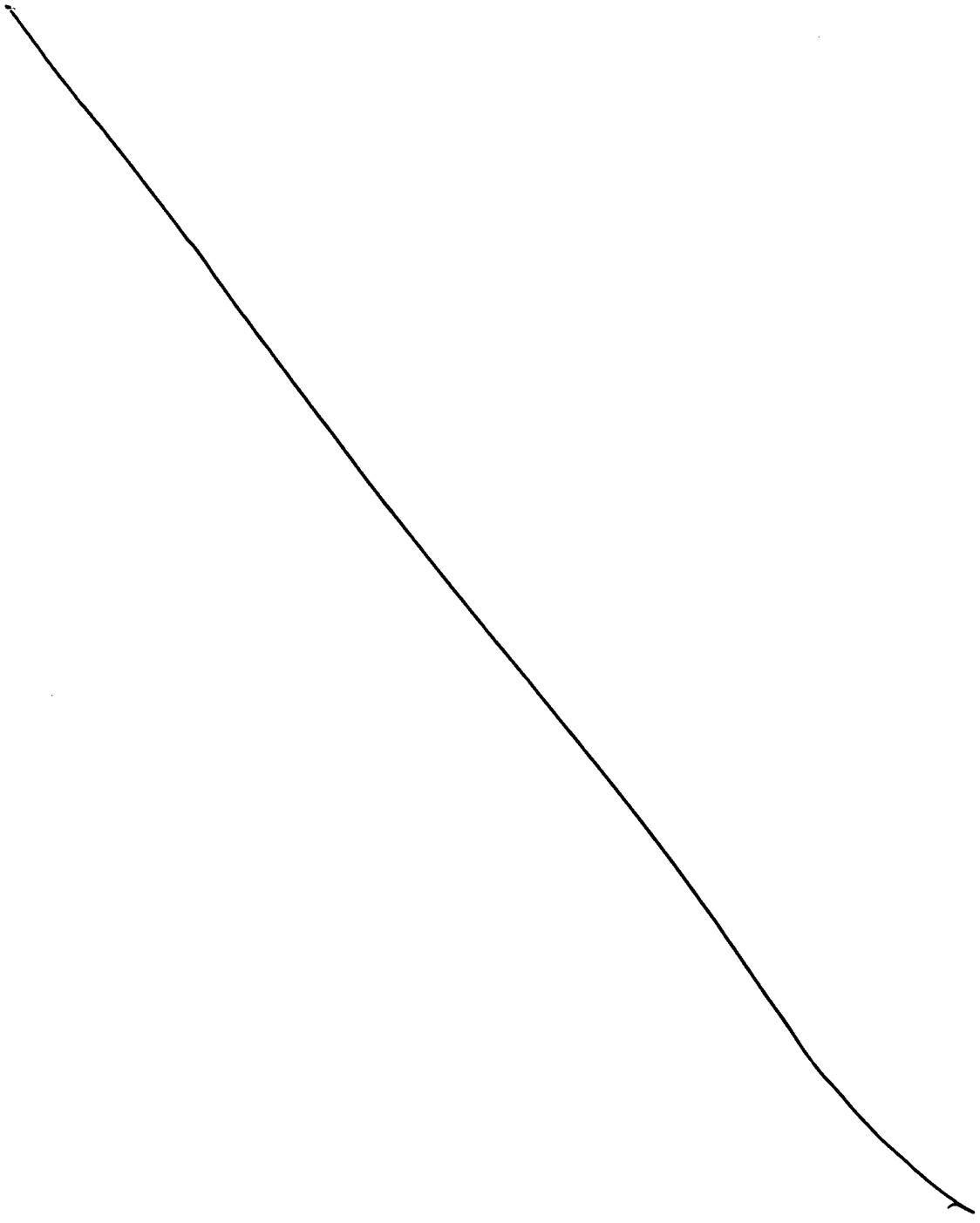
Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Urano et al. (US Patent No. 6,202,158) teaches a detection method of illegal access to computer system.

McNair (US Patent No. 5,559,505) teaches a security system providing lockout for invalid access attempts.

Kaufman et al. (US Patent No. 5,491,752) teaches a system for increasing the difficulty of password guessing attacks in a distributed authentication scheme employing authentication tokens.



Inquiries

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shahin Mizan whose telephone number is 571-272-0687. The examiner can normally be reached on M-F 8 a.m. - 4:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shahin Mizan
Examiner
Art Unit 2132

SM

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100